AMENDMENTS TO THE CLAIMS

1. (Currently Amended) An encryption apparatus for generating an encrypted text by encrypting a plaintext, said encryption apparatus comprising:

a storage unit operable to store an encryption key and a parameter, the parameter being adapted to a decryption apparatus and being used to change a probability of decryption error in decrypting the encrypted text;

an encryption unit operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in said storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter; and

an updating unit operable to update the parameter stored in said storage unit,

wherein the parameter stored in said storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on an NTRU encryption method, and

wherein said updating unit increases the number of the terms whose coefficients indicate 1 every passage of a predetermined amount of time.

2. (Canceled)

3. (Currently Amended) The encryption apparatus according to Claim [[2]] 1,

wherein said encryption unit generates the encrypted text using the encryption algorithm

based on ~~an~~ the NTRU encryption method.

4. (Canceled)

5. (Currently Amended) The encryption apparatus according to Claim [[4]] 1, further comprising:

an encryption key updating unit operable to receive, from the decryption apparatus, a request to update the encryption key, and to update the encryption key in response to the updating request; and

an initialization unit operable to receive, from the decryption apparatus, a request to update the number of the terms whose coefficients indicate 1 in the random number polynomial, and set, in response to the updating request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value.

6. (Previously Presented) The encryption apparatus according to Claim 5,

wherein said initialization unit sets the number of the terms whose coefficients indicate 1 in the random number polynomial to the initial value only when the decryption apparatus has paid a predetermined amount.

7. (Previously Presented) The encryption apparatus according to Claim 1,

wherein said updating unit updates the parameter stored in said storage unit so that the probability of the decryption error in decrypting the encrypted text increases with a passage of time.

8-9. (Canceled)

10. (Currently Amended) The encryption apparatus according to Claim 1,

wherein said encryption unit generates the encrypted text using an encryption algorithm based on ~~an~~ the NTRU encryption method.

11. (Canceled)

12. (Previously Presented) The encryption apparatus according to Claim 10,

wherein said encryption unit generates the encrypted text using the encryption algorithm used for the NTRU encryption method based on an EESS (Efficient Embedded Security Standard) method.

13. (Previously Presented) The encryption apparatus according to Claim 1, further comprising:

an encryption key updating unit operable to receive, from the decryption apparatus, a request to update the encryption key, and to update the encryption key in response to the updating

request; and

a parameter initialization unit operable to receive, from the decryption unit, a request to update the parameter, and set, in response to the initialization request, a value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value.

14-17. (Canceled)

18. (Currently Amended) An encryption system comprising an encryption apparatus for generating an encrypted text by encrypting a plaintext and a decryption apparatus for generating a decrypted text by decrypting the encrypted text,

wherein the encryption apparatus includes:

a storage unit operable to store an encryption key and a parameter, the parameter being adapted to the decryption apparatus and being used to change a probability of decryption error in decrypting the encrypted text;

an encryption unit operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in the storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter; and

an updating unit operable to update the parameter stored in the storage unit, ~~and~~ wherein the decryption apparatus includes:

a decryption unit operable to generate a decrypted text from the encrypted text using a decryption key;

a decryption key updating request unit operable to request the encryption apparatus to update the decryption key; and

a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value,

wherein the parameter stored in the storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on an NTRU encryption method, and

wherein the updating unit increases the number of the terms whose coefficients indicate 1 every passage of a predetermined amount of time.

19. (Canceled)

20. (Currently Amended) The encryption system according to Claim ~~19~~18,

wherein the encryption unit generates the encrypted text using an encryption algorithm based on ~~an~~ the NTRU encryption method ~~method,~~

~~the parameter stored in the storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption, and~~

~~the updating unit increases the number of the terms whose coefficients indicate 1 in the~~

~~random number polynomial after the passage of the predetermined amount of time~~.

21. (Original) The encryption system according to Claim 20,

wherein the decryption key updating request unit and the parameter initialization request unit respectively send, to the encryption apparatus, a request to update the decryption key and a request to initialize the parameter, together with a request to pay a predetermined amount, and

the encryption apparatus further includes:

a decryption key updating unit operable to receive, from the decryption apparatus, the request to update the decryption key, and update the decryption key in response to the updating request only when the predetermined amount is paid; and

an initialization unit operable to receive the request to initialize the parameter from the decryption apparatus, and set, in response to the initialization request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases a probability of decryption error to a value less than or equal to a predetermined value only when the predetermined amount is paid.

22. (Canceled)

23. (Currently Amended) The encryption system according to Claim 18,

wherein the encryption unit generates the encrypted text using the encryption algorithm based on ~~an~~ the NTRU encryption method.

24. (Currently Amended) The encryption system according to Claim 23,

~~wherein the parameter stored in the storage unit indicates the number of the terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption method,~~

wherein the decryption key updating request unit and the parameter initialization request unit respectively send, to the encryption apparatus, an instruction to update the decryption key and a request to initialize the parameter, together with a request to pay a predetermined amount, and

wherein the encryption apparatus further includes:

a decryption key updating unit operable to receive, from the decryption apparatus, the request to update the decryption key, and update the decryption key in response to the updating request only when the predetermined amount is paid; and

an initialization unit operable to receive the request to initialize the parameter from the decryption apparatus, and set, in response to the initialization request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases a probability of decryption error to a value less than or equal to a predetermined value only when the predetermined amount is paid.

25. (Original) The encryption system according to Claim 18,

wherein the decryption apparatus further includes a judgment unit operable to judge whether or not the decrypted text is obtained correctly,

the decryption key updating request unit instructs the encryption apparatus to update the

decryption key, according to a result of the judgment made by the judgment unit, and

the parameter initialization request unit instructs the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of decryption error to a value less than or equal to a predetermined value, according to the result of the judgment made by the judgment unit.

26. (Currently Amended) An encryption method for generating an encrypted text by encrypting a plaintext, said encryption method comprising:

an encrypted text generating step of generating the encrypted text from the plaintext, using an encryption key and a parameter, according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of the parameter adapted to a decryption apparatus; and

an updating step of updating the parameter,

wherein the parameter indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on an NTRU encryption method, and

wherein, in the updating step, the number of the terms whose coefficients indicate 1 is increased every passage of a predetermined amount of time.

27. (Previously Presented) The encryption method according to Claim 26,

wherein in the updating step, the parameter is updated so that the probability of the decryption error in decrypting the encrypted text increases with a passage of time.

28. (Canceled)

29. (Currently Amended) The encryption method according to Claim 26,

wherein in the encrypted text generation step, the encrypted text is generated using the encryption algorithm based on ~~an~~ the NTRU encryption method.

30-33. (Canceled)

34. (Currently Amended) A computer-readable storage medium on which an encryption program for generating an encrypted text by encrypting a plaintext is recorded,

wherein the encryption program causes a computer to execute a method comprising:

an encrypted text generation step of generating the encrypted text from the plaintext, using an encryption key and a parameter, according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of the parameter adapted to a decryption apparatus;

an updating step of updating the parameter; and

an outputting step of outputting the encrypted text,

wherein the parameter indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on an NTRU encryption method, and

wherein, in the updating step, the number of the terms whose coefficients indicate 1 is increased every passage of a predetermined amount of time.

35. (Canceled)

36. (New) The encryption apparatus according to Claim 1,

wherein the plaintext is a content including video and audio.

37. (New) The encryption apparatus according to Claim 1,

wherein the predetermined amount of time is one day.

38. (New) The encryption system according to Claim 18,

wherein the plaintext is a content including video and audio.

39. (New) The encryption system according to Claim 18,

wherein the predetermined amount of time is one day.

40. (New) The encryption method according to Claim 26,

wherein the plaintext is a content including video and audio.

41. (New) The encryption method according to Claim 26,

wherein the predetermined amount of time is one day.

42. (New) The computer-readable storage medium according to Claim 34,

wherein the plaintext is a content including video and audio.

43. (New) The computer-readable storage medium according to Claim 34, wherein the predetermined amount of time is one day.